NetBackup™ Web UI Oracle Administrator's Guide

Release 8.3

VERITAS™

NetBackup Web UI Oracle Administrator's Guide

Last updated: 2020-07-28

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1

Introducing the NetBackup web user interface

This chapter includes the following topics:

About the NetBackup web UI

The NetBackup web user interface provides the following features:

- Ability to access the master server from a web browser, including Chrome and Firefox.
  For details on supported browsers for the web UI, see the NetBackup Software Compatibility List.
- A dashboard that displays a quick overview of the information that is important to you.
- Role-based access control (RBAC) that lets the administrator configure user access to NetBackup and to delegate the tasks such as security, backup management, or workload protection.
- Management of NetBackup security settings, certificates, API keys, and user sessions.
- Protection of assets is achieved through protection plans, job management, and visibility of the protection status of assets. Alternatively, policy management is also available for a limited number of policy types.

- Workload administrators can subscribe assets to the protection plans that meet the SLO, monitor protection status, and perform self-service recovery of virtual machines. The web UI supports the following workloads:
  - Cloud
  - Microsoft SQL Server
  - Oracle
  - Red Hat Virtualization (RHV)
  - VMware
- Usage reporting tracks the size of backup data on your master servers. You can also easily connect to Veritas Smart Meter to view and manage NetBackup licensing.

Note: The NetBackup web UI is best viewed at a 1280x1024 or higher screen resolution.

Access control in the NetBackup web UI

NetBackup uses role-based access control to grant access to the web UI. Access control is accomplished through roles.

- A role defines the operations that a user can perform and the access that the user has to any workload assets, protection plans, or credentials. A user can have multiple roles, allowing for full and flexible customization of user access.
- RBAC is only available for the web UI and the APIs.
  Other access control methods for NetBackup are not supported for the web UI and APIs, with the exception of Enhanced Auditing (EA). You cannot use the web UI if you have NetBackup Access Control (NBAC) enabled.

Monitor NetBackup jobs and events

The NetBackup web UI lets administrators more easily monitor NetBackup operations and events and identify any issues that need attention.

- The dashboard displays an overview of NetBackup jobs, certificates, tokens, security events, and usage reporting.
  The dashboard widgets that display depend on a user's RBAC role and permissions.
- Email notifications can be configured so administrators receive notifications when job failures occur. NetBackup supports any ticketing system that can receive inbound email.

Protection plans: One place to configure schedules, storage, and storage options

Protection plans offer the following benefits:

- In addition to schedules for backups, a protection plan can also include a schedule for replication and long-term retention.
- When you select from your available storage, you can see any additional features available for that storage.
- With the necessary RBAC permissions, a workload administrator can create and manage protection plans, including the backup window and retention. See *NetBackup Web UI Administrator's Guide* for details on the roles permissions.
- A workload administrator can select the protection plans to use to protect assets or intelligent groups.

Self-service recovery

The NetBackup web UI makes it easy for a workload administrator to recover VMs or databases. For the workloads that support the instant access feature, users can mount a snapshot for immediate access to a VM's files or to a database.

Terminology

The following table describes the concepts and terms that are introduced with the new web user interface.

Table 1-1 Web user interface terminology and concepts

Term	Definition
Administrator	A user that has complete access and permissions to NetBackup and all of the interfaces, including the NetBackup web UI. The root, administrator, and Enhanced Auditing user all have complete access to NetBackup. In the *NetBackup Web UI* guides, the term *NetBackup administrator* also refers to a user that has full permissions for NetBackup. Usually in reference to a user of the NetBackup Administration Console. Also see *role*.
Asset group	See *intelligent group*.
Asset	The data to be protected, such as physical clients, virtual machines, and database applications.

Table 1-1 Web user interface terminology and concepts *(continued)*

Term	Definition
Backup now	An immediate backup of an asset. NetBackup performs a one-time, full backup of an asset using the selected protection plan. This backup does not affect any scheduled backups.
Classic policy	In the NetBackup web UI, indicates that a legacy policy protects the asset. Legacy policies are created with the NetBackup Administration Console.
External certificate	A security certificate that is issued from any CA other than NetBackup.
Intelligent group	Allows NetBackup to automatically select assets for protection based on the criteria (queries) that you specify. An intelligent group automatically stays up-to-date with changes in the production environment. These groups are also referred to as asset groups. For VMware and RHV, these groups appear under the tab **Intelligent VM groups**.
Instant access	An instant access VM or database that is created from a NetBackup backup image is available almost instantaneously, achieving a near-zero recovery time objective. NetBackup mounts the snapshot directly on the backup storage device and the snapshot is treated as a normal VM or database.
NetBackup certificate	A security certificate that is issued from the NetBackup CA.
Protection plan	A protection plan defines when backups are performed, how long the backups are retained, and the type of storage to use. Once a protection plan is set up, assets can be subscribed to the protection plan.
RBAC	Role-based access control. Administrators can delegate or limit access to the NetBackup web UI through the roles that are configured in RBAC. **Note:** The roles that you configure in RBAC do not control access to the NetBackup Administration Console or the CLIs. The web UI is not supported with NetBackup Access Control (NBAC) and cannot be used if NBAC is enabled.
Role	For RBAC, defines the operations that a user can perform and the assets or objects that they can access. For example, you can configure a role to mange recovery of specific databases and the credentials that are needed for backups and restores.

Table 1-1 Web user interface terminology and concepts *(continued)*

Term	Definition
Storage	The storage to which the data is backed up, replicated, or duplicated (for long-term retention).
Subscribe, to a protection plan	The action of selecting an asset or an asset group to subscribe to a protection plan. The asset is then protected according to the schedule in the plan. The web UI also refers to *Subscribe* as *Add protection*.
Unsubscribe, from a protection plan	*Unsubscribe* refers to the action of removing protection or removing an asset or asset group from a plan.
Workload	The type of asset. For example, VMware, RHV, or Cloud.
Workflow	An end-to-end process that can be completed using the NetBackup web UI. For example, you can protect and recover VMware and Cloud assets beginning with NetBackup 8.1.2.

Sign in to the NetBackup web UI

Authorized users can sign in to a NetBackup master server from a web browser, using the NetBackup web UI. The following sign-in options are available:

- Sign in with a user name and password
- Sign in with a certificate or smart card
- Sign in with single sign-on (SSO)

Sign in with a user name and password

Only authorized users can sign in to NetBackup web UI. Contact your NetBackup security administrator for more information.

To sign in to a NetBackup master server using a user name and password

1. Open a web browser and go to the following URL.

   https://*masterserver*/webui/login

   The *masterserver* is the host name or IP address of the NetBackup master server that you want to sign in to.

2. Enter your credentials and click **Sign in**.

   For example:

For this type of user	Use this format	Example
Local user	*username*	**jane_doe**
Windows user	*DOMAIN\username*	**WINDOWS\jane_doe**
UNIX user	*username@domain*	**john_doe@unix**

Sign in with a certificate or smart card

You can sign in to NetBackup web UI with a smart card or digital certificate if you are an authorized user. Contact your NetBackup security administrator for more information.

To use a digital certificate that is not on a smart card, you must first upload the certificate to the browser's certificate manager. See the browser documentation for instructions or contact your certificate administrator for more information.

To sign in with a certificate or smart card

1. Open a web browser and go to the following URL.

   https://*masterserver*/webui/login

   The *masterserver* is the host name or IP address of the NetBackup master server that you want to sign in to.

2. Click **Sign in with certificate or smart card**.

3. When your browser prompts you, select the certificate.

Sign in with single sign-on (SSO)

You can sign in to NetBackup web UI with the single sign-on (SSO) option if SAML is configured as an identity provider in your NetBackup environment. Contact your NetBackup security administrator for more information.

To sign in to a NetBackup master server using SSO

1. Open a web browser and go to the following URL.

   https://*masterserver*/webui/login

   The *masterserver* is the host name or IP address of the NetBackup master server that you want to sign in to.

2. Click **Sign in with single sign-on**.

3. Follow the steps as provided by your administrator.

   On subsequent logons, NetBackup signs you in automatically to the master server.

Sign out of the NetBackup web UI

Note that NetBackup automatically signs you out of the web UI after 24 hours, which is the maximum time that is allowed for a user session. After that time NetBackup requires that you sign in again. You can also sign out if you want to change the sign-in option that you want to use (user name and password, smart card, or single sign-on (SSO)).

To sign out of the NetBackup web UI

- On the top right, click the profile icon and click **Sign out**.

Chapter 2

Managing Oracle

This chapter includes the following topics:

About Oracle discovery

The NetBackup Discovery Service (`nbdisco`) discovers Oracle database instances throughout the NetBackup environment. The discovery service reports to the master server when it finds instances and databases to help you build an Oracle Intelligent Policy. The service polls the clients upon NetBackup installation and periodically after installation (every 4 hours). Instance management collects the discovered instances in an instance repository. The user can access this repository on the NetBackup web UI or by using the `nboraadm` command.

The NetBackup Discovery Service searches for instances and databases in different areas where Oracle is installed. The following areas are where the Discover Service searches:

- Non-RAC Single instances are discovered by searching the `oratab` file on UNIX and from the registry on Windows.
- NetBackup looks for the Oracle health check files that are found in the Oracle home. These are not cleaned up when a database is deleted. You may need to delete them manually otherwise NetBackup can continue to find the databases that are deleted.
- Oracle RAC databases are discovered when NetBackup queries the Oracle Cluster Ready Services (CRS) using the Oracle Clusterware high availability API.

Oracle RAC in the web UI does not support upgrades from legacy script-based policies. Also, there is no web UI support for the configurations that are created using Appendix A or Appendix B in the NetBackup for Oracle Administrator's Guide.

To allow the NetBackup web UI to discover a RAC instance or cluster:

- Remove the Oracle RAC from any configuration that is setup using Appendix A or Appendix B in the NetBackup for Oracle Administrator's Guide.
- Remove any Oracle RAC from existing OIP policies in the current NetBackup Administrator's Console.

Note: When an Oracle RAC database is discovered, that database does not have a **Database ID**. A **Database ID** is required to manually add additional RAC instances to the database. You must register the RAC database and provide a **Database ID** before adding additional instances.

See "Manage credentials for an instance or an Oracle RAC database" on page 18.

See "Add an Oracle Real Application Cluster (RAC)" on page 16.

By default, this service is enabled to report instances. However, you can use the `REPORT_CLIENT_DISCOVERIES` client configuration entry to shut down or restart the service on a particular client. By default, `REPORT_CLIENT_DISCOVERIES` is not present in the Windows registry or the UNIX `bp.conf` file.

To change the default setting, use `bpsetconfig` to add or change the entry:

- In the Windows registry.
- In the `/usr/openv/netbackup/bp.conf` file on UNIX.

Use the following format: `REPORT_CLIENT_DISCOVERIES = TRUE | FALSE`

Set `REPORT_CLIENT_DISCOVERIES` to `FALSE` to shut down the discovery service. The service shuts down within 10 minutes and remains down on the client. To turn on the discovery service on that client, set `REPORT_CLIENT_DISCOVERIES` to `TRUE`or remove the entire entry. Then run `bp.start_all` on the client to restart the service.

To set this value on a client remotely, run the following command from the master server:

```
echo REPORT_CLIENT_DISCOVERIES=FALSE | bpsetconfig -h clientname
```

Add an Oracle instance

In NetBackup, you can manually add an instance or allow NetBackup to scan for any Oracle instances. The NetBackup Discovery Service (`nbdisco`) discovers Oracle database instances throughout the NetBackup environment. All of the instances that are manually added or NetBackup discovers are populated in the **Instance** tab table.

Note: For more information about instance management, see *Instance management for an Oracle Intelligent Policy* in the NetBackup for Oracle Administrator's Guide.

To manually add an instance

1. On the left, click **Workloads** > **Oracle** and then click **Instances**.
2. In the **Instances** tab, click **Actions** and select **Add instance**.
3. Enter the required information for the instance.
4. (Optional) Enter the **Override default TNS_ADMIN path**if you need to override the default network administration directory on the client system. Enter the fully qualified path for the network administration directory on this host.
5. After all the required information for instance is entered, you can:
   - Click **Finish** to add the instance. Select this option to add the instance to NetBackup without credentials. The credentials can be added at a later time.
   - Click **Add and manage credentials** to add credentials for the instance at this time.

     In the **Manage credentials for instance** screen, select one of the appropriate credential authentication methods:

     - Select **Add to group and register using group credentials** to register the instance using group credentials. Select the instance group name from the drop-down.
     - Select **Use instance credentials** to register using the instance credentials. Select the credential option for this instance and enter all required information.

     Click **Finish** to add this instance with credentials.

To add an instance with the Discovery option

1. On the left, click **Workloads** > **Oracle** and then click the **Instances** tab.
2. In the **Instances** tab, click **Actions** and select **Discover instances**.
3. Click **Start discovery**.
4. Add credentials for the instance per step 5

Add an Oracle instance group

NetBackup lets you create an instance group that includes instances with a common set of credentials. You can create a default instance group for newly-discovered instances. Oracle RAC databases cannot be added to an instance group.

To add an Oracle instance group

1. On the left, click **Workloads** > **Oracle** and then click **Instance groups**.
2. In the **Instance groups** tab, click **Actions** and select **Add instance group**.
3. Enter the required information.
4. Enter the credential information for the **Instance credentials** option you select.

   The credential options change based on the option that is selected in **Instance credentials**.
5. Click **Finish**.

See "Add an Oracle instance" on page 14.

See "Add an Oracle Real Application Cluster (RAC)" on page 16.

Clean up Oracle instance and databases

NetBackup can automatically remove orphaned instances and databases if they are not registered or are no longer discoverable. Orphaned instances are the databases that were discovered at one time but were never registered. This operation is done automatically once you set the number of days.

To set up automatic cleanup of instances

1. On the left, click **Workloads** > **Oracle** and then click **Instances**.
2. In the **Instances** tab, click **Actions** and select **Instances cleanup**.
3. Set the number of days and then click **Cleanup**.

See "Add an Oracle instance" on page 14.

See "Add an Oracle Real Application Cluster (RAC)" on page 16.

See "Edit or delete an Oracle RAC database" on page 17.

Oracle Real Application Clusters (RAC)

In a Real Application Clusters (RAC) environment, many Oracle database instances exist on separate servers, each with direct connectivity to a single Oracle database. All the servers can run transactions concurrently against the same database. Should any single server or instance fail, processing continues on the surviving servers.

RAC supports all Oracle backup features that are available in exclusive mode, including online backups and offline backups of an entire database or individual tablespaces.

Currently, only the NetBackup web UI has full RAC support for Oracle policies. This manual contains only the information that is needed to add an Oracle RAC to the web UI.

To manage classic policies you must use the NetBackup Administration Console. However, Oracle policies protecting an Oracle RAC can be managed in the NetBackup web UI. See the NetBackup for Oracle Administrator's Guide for full details on creation and management of an Oracle policy.

Note: Any nodes of the Oracle RAC cluster that is used in backups, must be running a NetBackup client. The version should be the same version across the cluster. For Oracle RAC OIP support the NetBackup 8.3 client is required.

Add an Oracle Real Application Cluster (RAC)

Use this procedure to add an Oracle RAC and the appropriate credentials. Once an Oracle RAC is added, you can create a policy in the web UI to schedule a backup of the Oracle RAC.

Add an Oracle RAC

1. On the left, click **Workloads** > **Oracle** and then click **RAC databases**.
2. In the **RAC databases** tab, click **Actions** and select **Add RAC**.
3. Enter all the required information for the Oracle RAC database and then click **Next**.
4. Enter all the required information for an Oracle RAC instance and then:
   - Click **Finish** to add the Oracle RAC and the instance. Select this option to add the RAC to NetBackup without credentials. The credentials can be added at a later time.

- Click **Add and manage credential** to add credentials for the Oracle RAC database at this time. Choose the credential option for this RAC:
  - **Use Oracle Wallet**. Enter the Oracle Wallet folder location. The folder location must be on a file system.

    Using Oracle Wallet requires these items:
    - The same path for each node of the cluster.
    - Each instance must have its own entry in a shared wallet.
    - You must put a specific connection identifier in the wallet.
      For more information about the connect identifier:
      See "Configure an Oracle Wallet with RAC within NetBackup" on page 20.
    - A single instance must have the path to the wallet and the Net service name (TNS alias).
  - **RAC database credentials**. Enter a user name and password.
  - **Use Oracle RMAN recovery catalog**. Select this option and enter a user name, password, and the Net service name (TNS alias). This option can be used with Oracle Wallet but it must be the same wallet as the database connection.

  Enter the appropriate credential information for the Oracle RAC and then click **Add credentials**.

See "Load balance Oracle RAC instances" on page 19.

See "Add an Oracle instance" on page 14.

Edit or delete an Oracle RAC database

Edit an Oracle RAC database

Use this procedure to edit the information that is entered for the Oracle RAC database.

Edit an Oracle RAC database

1. On the left, click **Workloads** > **Oracle** and then click **RAC databases**.
2. In the **RAC databases** tab, click the Actions menu for the RAC and select **Edit**.

   Also, you can click **Edit RAC database** on the top right of the page when viewing the **Oracle RAC database** details page.

3 Enter the required information and then click **Next**.

Changing the **RAC type** is optional when editing an Oracle RAC.

Editing the **Backup host** is optional.

You cannot edit the **Database unique name** or the **Database ID**.

4 Enter the required information and then click **Save**.

Delete an Oracle RAC database

Use this procedure to delete an Oracle RAC.

Delete an Oracle RAC database

1 On the left, click **Workloads** > **Oracle** and then click **RAC databases**.

2 In the **RAC databases** tab, click the Actions menu for the Oracle RAC database and select **Delete**.

3 Click **OK**.

See "Add an Oracle Real Application Cluster (RAC)" on page 16.

See "Add an Oracle instance" on page 14.

See "Clean up Oracle instance and databases" on page 15.

Manage credentials for an instance or an Oracle RAC database

You can add or update credentials for instances and RAC databases at any time. When you manually add an instance or a RAC database, you can choose not to include the credentials at time of entry. After the discovery service adds new instances and RAC databases to the repository, you can add credentials. NetBackup provides a way to enter the proper credentials for your instance and RAC databases.

When an Oracle RAC database is discovered, that database does not have a **Database ID**. A **Database ID** is required to manually add additional RAC instances to the database. You must register the RAC database and provide a **Database ID** before adding additional instances.

To add credentials for an instance

1 On the left, click **Workloads** > **Oracle** and then click **Instances**.

2 In the **Instances** tab, click the Actions menu for the instance and select **Manage credentials**.

3 In the **Manage credentials for instance** screen, select one of the appropriate credential authentication methods:

- Select **Add to group and register using group credentials** to register the instance using group credentials. Select the instance group name from the drop-down.
- Select **Use instance credentials** to register using the instance credentials. Select the credential option for this instance and enter all required information.

4 Click **Finish**.

To add credentials for a RAC database

1 On the left, click **Workloads** > **Oracle** and then click **RAC databases**.

2 In the **RAC databases** tab, click the Actions menu for the instance and select **Manage credentials**.

3 In the **Manage credentials for RAC database** screen, select one of the appropriate credential authentication methods:

- Select **Use Oracle Wallet** to use the credentials that are located in the Oracle Wallet. For non-RAC installations, the instance net service name must be stored in the Oracle Wallet as defined in Oracle's wallet documentation.
- Select **RAC database credentials** and enter the correct **User name** and **Password** for the database.
- (Optional) Enter credentials for the **Oracle RMAN recovery catalog credentials** section.

4 Click **Add credentials**.

Load balance Oracle RAC instances

NetBackup can be set up to load balance the instances that makeup the Oracle RAC. Use this feature to distribute the backup load across all of the instances and to exclude any Oracle RAC instances from the backup.

To load balance Oracle RAC instances

1 On the left, click **Workloads** > **Oracle** and then click **RAC databases**.

2 In the **RAC databases** tab, click the Actions menu for the Oracle RAC database and select **Load balance**.

3 In the **Select number of instances to load balance**, select the number of instances to include for load balancing.

If you select **All**, all instances in the Oracle RAC are available for load balancing.

4 In the table, select the instance or instances you want to move up or down in priority.

5 Click **Move up** or **Move down** to move the instances.

Click **Move up** to move the instance or instances to the top of the list.

Click **Move down** to move the instance or instances to the bottom of the list.

6 (Optional) If you select **Do not use** in the action menu on the right, that instance moves to the **RAC instances excluded from backup** table.

NetBackup does not use this instance when backup operations are performed.

7 Click **Save**.

See "Add an Oracle Real Application Cluster (RAC)" on page 16.

Configure an Oracle Wallet with RAC within NetBackup

The configuration and setup of the Oracle Wallet in NetBackup is a two-step process. You add descriptors first, then you register the wallet. In the cases of Oracle RAC, your descriptors must enumerate the list of RAC instances that comprise your RAC cluster.

NetBackup Oracle Wallet prerequisites:

- The Oracle wallet location must be accessible from all nodes of the RAC cluster.
- Using a shared location is encouraged for maintainability.
  An example storage location can be: An Oracle ACFS file system that is mounted on each node or an NFS share accessible to each node. The mount point of the shared location must be the same on each node.
- If the wallet is not in a shared location, it must be in an identically duplicate location on each node of the RAC cluster. The full contents of the wallet must also be duplicated on each node of the RAC cluster.

To configure Oracle Wallet with RAC in NetBackup:

1 On the left, click **Workloads** > **Oracle** and then click **RAC databases**.

2 Click on the **Database name** of the RAC you want to configure and view the details.

Copy the **Scan name**, **Service name**, and **Port**.

To view the details of the RAC from the CLI, run `nboraadm -list_rac_dbs`.

3. Copy the RAC instance names of the discovered instances.

   To view the RAC instance names of the discovered instances from the CLI, run `nboraadm -list_rac_instances`.

4. Create the connect descriptors for insertion into wallet using the information that is gathered in step 2 and step 3.

   Example connect descriptors:

   ```
   (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
   (HOST=<INSERT SCAN NAME>)(PORT=<Port number>))
   (CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=<INSERT SERVICE NAME>)
   (INSTANCE_NAME=<INSERT INSTANCE 1 NAME>)))
   ```

   ```
   (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
   (HOST=<INSERT SCAN NAME>)(PORT=<INSERT PORT>))
   (CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=<INSERT SERVICE NAME>)
   (INSTANCE_NAME=<INSERT INSTANCE 2 NAME>)))
   ```

   You must create connect descriptors for each of the RAC instances in the wallet.

5. Add the connect descriptors with the Oracle `MKSTORE` utility. The descriptors are case-sensitive and must match exactly to what is in NetBackup.

   ```
   mkstore -wrl /db/orac183/wallet/ -CreateCredential
   '(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=exampleScanName.veritas.com)
   (PORT=1521))(CONNECT_DATA=(SERVER=DEDICATED)
   (SERVICE_NAME=orac183.veritas.com)(INSTANCE_NAME=orac1831)))'
   testUser testPassword
   ```

   ```
   mkstore -wrl /db/orac183/wallet/ -CreateCredential
   '(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=exampleScanName.veritas.com)
   (PORT=1521))(CONNECT_DATA=(SERVER=DEDICATED)
   (SERVICE_NAME=orac183.veritas.com)(INSTANCE_NAME=orac1832)))'
   testUser testPassword
   ```

6 Register the RAC with the wallet path in using the web UI.

See “Add an Oracle Real Application Cluster (RAC)” on page 16.

To register the RAC with the wallet path from the CLI, run `nboraadm -register_rac_db`.

If the RAC is registered for the first time from discovery, you need to include the `dbid`. From the CLI, run `nboraadm -register_rac_db -rac_db_unique_name`.

7 (Optional) If you get an error when you attempt to register the RAC, review the error message. Compare the descriptors in the error message with what you generated in step 4 and what you inserted into your Oracle wallet.